Commonwealth Office
of
Technology
Monthly Cyber Security Tips

December 2009 Volume 4, Issue 12

Automatic Software Updates and Patching

From the Office of COT's Chief Information Security Officer

Security vulnerabilities are flaws in the software that could allow someone to potentially compromise your system. Each year, the volume of software security vulnerabilities discovered increases, and the hacking tools available to exploit these vulnerabilities become more readily available and easier to use. Vulnerabilities in commonly used programs such as Adobe PDF Reader, QuickTime, Adobe Flash and Microsoft Office are prime targets of attacks on computers connected to the Internet. Recent statistics reported show that 48% of the cyber attacks identified in the second quarter of 2009 were targeted against vulnerabilities in Adobe Acrobat/Adobe Reader[1] and in October 2009 Microsoft released patches for a record number of security holes. No entity is immune to vulnerabilities, so we must ensure we understand the risks and take appropriate mitigation steps.

Why do I need to update my software?

One of the basic tenets of computer security is to update your operating system and other software installed on your computer. Software updates fix problems in the software, add functionality, and most importantly, fix vulnerabilities that impact the security of the software and subsequently your computer. These vulnerabilities can lead to your computer—and information that resides on it—being compromised. Exploitation of vulnerabilities may occur by opening documents, viewing an email which contains malicious code or visiting a web site hosting malicious content. Seventy percent of the top 100 web sites hosted malicious content or contained a link designed to redirect users to malicious sites.[2]

What is a software patch (fix) and when should I install software patches?

Patches are often called "fixes." A patch is software that is used to correct a problem to an application (software program) or an operating system. Computer companies are continuously addressing security holes (i.e. vulnerabilities) in computer software which could be used to infect your computer with a virus, spyware or worse. When vulnerabilities are discovered, the software vendor typically issues a fix (i.e. patch) to correct the problem. This fix should be applied as soon as possible since the average time for someone to try to exploit this security hole can be as little as a few minutes. Most major software companies will periodically release patches, usually downloadable from the Internet, that correct very specific problems in their software programs.

My computer has dozens of software programs -- which ones should I update and how often?

One of the challenges facing the average computer user is to know which software needs to be updated and how often. Software programs that communicate or interact with the Internet are especially susceptible to attacks and should be kept at a vendor-supported version and current on all patches.

Many software programs include a feature called "auto update." This feature allows the computer to check for updates at periodic intervals. The software will automatically check for updates and save them to your computer. Some updates will instruct you to "reboot" your computer before the software update can be applied.

At a minimum, you should enable the auto update feature on the following products:

- **Anti-virus and Anti-spam signatures**: anti-virus and anti-spam software requires regular updates to virus and spam signatures to remain effective. New viruses and other types of malware appear every day

and the anti-virus/anti-spam vendors release new signatures on a daily basis to stay on top of the new threats.

- **Windows Office software:** Word, Excel, Outlook, etc. – (see below for updating Windows software)
- **Internet Browsers:** e.g., Internet Explorer (Microsoft), Firefox (Mozilla), Safari (Apple) and Chrome (Google). Make sure you update any software you use for browsing the Internet.
- **Adobe products:** e.g., Adobe Reader, Adobe Acrobat, Flash, Shockwave
- **Media Players:** e.g., Windows Media Player (Microsoft), QuickTime (Apple), Real Player (Real Networks) and Flash Player (Adobe)
- **Java (Sun Microsystems)**: Java is software that is installed on most computers to allow users to play online games, conduct online chats, and view images in 3D, among other functions. It is also used for Intranet applications and other e-business solutions.
- **Other software programs that communicate or interact with the Internet**, like e-mail, web servers, and remote desktop software are especially susceptible to attacks and should be kept current on patches and version levels.

It is very important to promptly download and patch your operating system and programs whenever security updates or "service packs" become available. These patches are created to protect systems against potential attacks. Be aware that attacks sometimes occur before updates are released.

How do I update my Microsoft Windows programs?

Windows Update is a Microsoft service that provides updates for the Windows operating system and other Microsoft software. Installing Windows updates, such as "service packs" and other patches, is necessary to keep your Windows system secure. To activate Windows Update, go to Settings/Control Panel/Automatic Updates. When you turn on Automatic Updates, Windows routinely checks the Windows Update web site for high-priority updates that can help protect your computer from the latest viruses and other security threats. These updates can include security updates, critical updates, and "service packs." Depending on the setting you choose, Windows automatically downloads and installs any high-priority updates that your computer needs, or notifies you as these updates become available. Be sure to set the auto updates to daily, as patches can be released at any time.

Note*: *Many organizations have formal processes to patch systems that will automatically update all appropriate software. In these situations, no end user action is required.

****

Source: 1. F-Secure
Source: 2. SC Magazine

Online Resources

To learn more about protecting information visit the following online resources:

- **MS ISAC Monthly Cyber Security Tips**: www.msisac.org/awareness/news
- **US CERT**: www.us-cert.gov/reading_room
- **OnGuard Online**: www.onguardonline.gov/topics.html
- **Privacy Rights Clearinghouse**: www.privacyrights.org

For more cyber security monthly tips go to:
www.msisac.org/awareness/news/
technology.ky.gov/security/CyberAwareness.htm

Brought to you by:

MS-ISAC
www.msisac.org

COT
technology.ky.gov